

Sep 24, 2020

s/ Daryl Olszewski

Deputy Clerk, U.S. District Court  
Eastern District of Wisconsin

## UNITED STATES DISTRICT COURT

for the  
Eastern District of Wisconsin

In the Matter of the Search of

*(Briefly describe the property to be searched  
or identify the person by name and address)*MEGA's downloaded digital content of Beck's MEGA  
account – Macgwire532@gmail.com located at the FBI  
Milwaukee Office located at 3600 S. Lake Drive, St. F

Case No. 20 MJ 203

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section  
18 U.S.C. § 2252A

Offense Description

The application is based on these facts:

See attached affidavit.

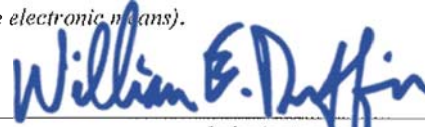
- ☐ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days *(give exact ending date if more than 30 days: \_\_\_\_\_)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Dickson Woo, Task Force Officer, FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by  
telephone \_\_\_\_\_ *(specify reliable electronic means)*.Date: September 24, 2020

Judge's signature

City and state: Milwaukee, Wisconsin

William E. Duffin, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Dickson Woo, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that is stored at premises owned, maintained, controlled, or operated by MEGA, Limited an online, electronic file storage provider headquartered at Level 21, Huawei Centre 120 Albert St Auckland 1010 New Zealand. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require MEGA, Limited. to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications.

2. I am a Task Force officer with the Federal Bureau of Investigation (FBI), and have been since January, 2015 I am assigned to the FBI's Child Exploitation Task Force, Milwaukee Division. My duties include investigating violations of federal criminal law, including violations of Title 18, United States Code, Section 2252, which criminalizes accessing with intent to view, possession, receipt, and distribution of child pornography. I have gained experience in conducting these investigations through training and through everyday work, to include executing search warrants and conducting interviews of individuals participating in the trading and manufacturing of child pornography. I have also received training relating to the investigation of Internet Crimes against Children (ICAC) which includes training in the investigation and enforcement of state and

federal child pornography laws in which computers and other digital media are used as a means for receiving, transmitting, and storing child pornography.

3. As a Federal Task Force officer, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States. In particular I investigate violations of Title 18, United States Code, Sections 2251 and 2252A which criminalize, among other things, the production, advertisement, possession, receipt, and transportation of child pornography.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 2252A have been committed by Macgwire Beck. There is also probable cause to search the information described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

#### **PROBABLE CAUSE**

6. The FBI had identified Kik user "KitB10" as a person sharing, posting, and trading images of child pornography on Kik. This Kik user "KitB10" was later identified as DAXTON HANSEN ("Hansen"), an adult male, living in Roy, Utah.



7. On 04/12/2017 a search warrant was executed at Hansen's residence in Roy, Utah. Multiple digital devices were seized which belonged to Hansen. Hansen admitted he had been viewing and sharing child pornography for approximately two years on Kik. He primarily shared, stored, and viewed child pornography via the application Kik. Hansen used the Kik profile name "KitB10" and only used this profile to share child pornography. Hansen was communicating with hundreds people on Kik and was an "Administrator" to multiple child pornography groups in Kik. All of these groups traded nude images or videos of young prepubescent boys engaged in various sexual acts. Hansen and other Kik users he communicated with frequently traded child pornography via Dropbox, pCloud, and other online or cloud based storage. Hansen estimated that he primarily sought child pornography images or videos of young boys ages 8-11. During the interview Hansen also signed an FD-1086, "Consent to Assume Online Identity Authorization" form for his Kik and Instagram accounts.

8. **Account Takeover of "KitB10": Online Undercover Session Summary**

Date Beginning/Ending: 04/12/2017 to Current

Software/Application: KIK Messenger Application

9. **Session Details:**

Online Covert Employee - 6765 ("OCE") was connected to the Internet in an online undercover capacity from a computer located at the FBI Office in Salt Lake City. A software program "Camtasia Studio" was used to record the online activity, chats, and child pornography identified within Kik.

10. Beginning on 04/12/2017 and continuing until current, OCE signed onto the internet in an undercover capacity and initiated Kik instant messenger using the Kik username

"KitB10" - (Access to this screen name had been provided via consent during the interview of Daxton Hansen). Hansen used this profile to create numerous child pornography groups, which he would facilitate finding people to add to the group, encourage others to trade or produce child pornography, and ban users from the group who wouldn't share or trade. A Kik user can create their own screen name and username. The username within their profile stays the same while the screen name can be changed at any time. The following was accomplished during these online undercover sessions:

11. On 04/12/2017, OCE identified numerous Kik Groups and hundreds of Kik contacts who were actively trading images of nude prepubescent aged children (boys and girls) engaged in numerous sex acts. Some of the child pornography Kik Groups that "KitB10" was member of were titled "The Loony Bin", "Boy Links Only! Send On Entry Or Ban", "Gaypervyoung", "Lovely Boys", "Boy Group", "Boy Poorn Lovers", "Trade", "Trade DB", "DBT", "Dropbox or other" and etc. Each group can contain up to 50 members. Over the course of the online undercover session, members would be invited and/or banned from the group by the administrators if they were not posting images and videos of child pornography. Most of the Kik groups required Kik users to post child pornography to the group before entry was allowed. Through OCE's training and experience, administrators of these groups find other people within Kik who have previously shared or shown interest in child pornography. These Kik users were then invited to the group. The administrators only invited members who will post images of child pornography and they will encourage other members to share images and videos. OCE did not have access to any previously posted images, videos, and/or comments prior to the OCE's account takeover.

12. OCE reviewed the messages, pictures, and videos posted by members of these child pornography groups and observed numerous videos, pictures, and links depicting child pornography, as well as comments posted by others in response to images and videos of child pornography that were posted. Images and videos posted to these groups depicted prepubescent boys posing in various stages of undress in sexually explicit positions and videos of children engaging in sexual activity with adults or children. Every member of the Kik group has the ability to post, view, and download images within the group. Every time the OCE identified a Kik member posting images of child pornography recordings were taken of the member's profile and profile image. The images or videos posted were downloaded or recorded for evidence. "Camtasia Studio" was used to record the videos and chat messages posted by the members.

13. KIK Messenger ("Kik") is a free chat application for mobile devices in which users can send text messages, pictures, and videos to other users. Kik users can communicate directly with an individual or with multiple users in a group chat. When signing up for a Kik account, a user supplies an email address, a unique username, and a display name that is seen when chatting with other users. On 04/28/2017 to 05/22/2017 OCE identified that Kik user "no\_limits\_bmx", was a member of a known child pornography group within Kik titled "Boy Links Only! Send on Entry or be Kicked". This group distributed, advertised, facilitated, discussed, accessed, viewed, and/or downloaded thousands of videos and images of child pornography.

14. The Kik user "no \_limits\_bmx" did post child pornography via Dropbox "links" on 04/30/2017 and 05/14/17 and was a member of the group for almost a month where thousands of images/videos of child pornography were shared. Most of the images/videos shared by members



in the group were nude prepubescent and toddler age boys engaged in sexual acts with adults and other children.

15. During a Kik chat on 04/30/17 “no\_limits\_bmx” posted the following dropbox link:

[https // www.dropbox.com/sh/1jdp2fq9dib7yim/AADrIVab9a5dFnCHUgx14-ZHa?dl=0](https://www.dropbox.com/sh/1jdp2fq9dib7yim/AADrIVab9a5dFnCHUgx14-ZHa?dl=0)

and on a another Kik chat on 05/14/17 “no\_limits\_bmx” posted a dropbox link:

[https://www.dropbox.com/sh/z478vn7nlkavsbC/AAB6\\_kn3l32iWeGwACclQlsea?dl=0](https://www.dropbox.com/sh/z478vn7nlkavsbC/AAB6_kn3l32iWeGwACclQlsea?dl=0)

OCE had clicked on the dropbox link from the 04/30/17 posting and observed a zip file named “Cold Sweat.zip”. OCE then opened the zip file and observed 89 videos. OCE also downloaded the zip file with the 89 videos. According to OCE some of the videos were child pornography videos. I reviewed the videos and determined that 7 of the videos appeared to be child pornography videos.

16. One of the video titled: File Feb 24, 11 46 37 PM.mp4 was a 35 second video of an adult performing a penis to anus sex act with a 6 to 15 month old infant.

17. On 05/03/2017, an Administrative Subpoena was served on Kik requesting subscriber information associated with username “no\_limits\_bmx”. On 07/17/2017, Kik responded and provided the following information:

Username: no\_limits\_bmx

First name: Macgwire

Last name: middle finger..middle finger

Email: macgwire536@yahoo.com (unconfirmed)

IP Address: 99.19.101.187

18. A query on the IP address 99.19.101.187 was conducted through the American Registry for Internet Numbers (ARIN) showed it was listed to AT&T.

19. On 08/14/2017, an Administrative Subpoena was served on AT&T requesting subscriber information associated with the IP address 99.19.101.187 provided by Kik. On 08/18/2017, AT&T responded and provided the following information:

Name: E M

Account #: 149804026

Address: 4xx Courtland Ave, Oshkosh, WI 54901-9736

Email address: Skulinu83@aol.com

Phone #: (716) 466-xxxx

20. On 12/08/17, an Administrative Subpoena was served on Yahoo requesting subscriber information associated with the email address of Macgwire536@Yahoo.com provided by Kik. On 12/11/17, Yahoo responded and provided the following information:

There is no such email address on record

21. A check in open source records showed a Macgwire J. Beck resided at the address listed in the AT&T subpoena (425 Courtland Ave, Oshkosh, WI) and related to E M (Beck). A comparison of the Wisconsin department of motor vehicle (DMV) driver's license photo of Macgwire J. Beck (M/W 06/09/xx) matched the photo for the Kik profile of "no\_limits\_bmx\_"



and the Kik name “Macgwire”. The DMV record also listed Macgwire Beck with the same listed address of 425 Courtland Ave, Oshkosh, WI.

22. Upon receipt of this information, the suspected user of Kik name of “no\_limits\_bmx” was identified as Macgwire J. Beck (white male 5’4”, 135 lbs; DOB: 06/09/xxxx; SSN: xxx-xx-4037; Wisconsin driver's license: B200-5509-xxxx-xx of 4xx Courtland Ave, Oshkosh, WI 54901-9736.

23. On December 15, 2017 a Search warrant was approved and sent to Dropbox, Inc for the content of Macgwire Beck’s account. On December 19, 2017 TFO Woo received the record from Dropbox, Inc regarding the Macgwire Beck’s account. A review of the account information revealed that in the account activity records that Beck did download the series of videos in the “Cold Sweat” folder three times. The first download was on February 28, 2017 (98 files) and then deleted on May 2, 2017. The second download was on June 7, 2017 (145 files) and deleted on June 10, 2017. The third time it was downloaded on June 11, 2017 (27 files) and deleted on September 21, 2017.

24. The Dropbox records also showed Macgwire Beck’s Dropbox account was registered under the email address of macgwire53@gmail.com and User ID: 337525966.

No Child pornography was located in the downloaded files in Beck’s dropbox account.

25. On July 10, 2018 it was determined that Beck had moved out of his parent’s residence at 4xx Courtland Ave, Oshkosh, WI and into another residence at 15xx Henry Street, Neenah, WI. Beck’s WI driver’s license showed he updated his address on June 27, 2018.

26. On July 24, 2019 FBI SA Elliot Mustell and TFO Dickson Woo met Macgwire Beck at his employment located at American paper converters 5xx Bondow Dr, Neenah, WI for an interview. During the interview Beck admitted to that he was on KIK and chatting with people that were trading images of children under the age of 18 years old in sex acts. Beck also admitted to asking underage boys and girls for nude images while in the KIK chat rooms. Beck then admitted to having child pornography in his MEGA account in 2018. Beck stated the account was closed due to breach of service. Beck had given us his account user name as Macgwire53@gamil.com or Macgwire532@gamil.com and several possible passwords. SA Mustell attempted to access the account during this interview but the MEGA account was not accessible due to the account being closed.

27. On January 30, 2020 TFO Woo forwarded the MEGA user names and passwords to FBI Staff operational specialist (SOS) Hannah Judd. SOS Judd then contacted the New Zealand government that has access to MEGA account information and forwarded the information to them so they could access the contents of Beck's MEGA account. TFO Woo was informed that MEGA has given access to their records to a select amount of people that work in the New Zealand government specifically for cases involving Sexual Exploitation of Children matters.

28. On January 31, 2020 TFO Woo received information from SOS Judd that approximately 40 GB of data was being sent to the Milwaukee FBI office for Beck's MEGA account. The data was received and downloaded to a computer in the FBI Milwaukee – Child Exploitation Task Force office located at 3600 S. Lake Drive, St. Francis, WI 53235, Room 3260 “Innocent Images”.

29. Mega is a cloud storage and file hosting service produced by Mega Limited. The New Zealand-based website was launched on 19 January 2013 by Kim Dotcom. Mega mobile apps are available for Windows Phone, Android, BlackBerry OS and iOS.

30. “MEGA” refers to an online storage medium on the internet accessed from a computer or electronic storage device. As an example, online storage mediums such as MEGA make it possible for the user to have access to saved files without the requirement of storing said files on their own computer or other electronic storage device. MEGA is an “offsite” storage medium for data viewed at any time from any device capable of accessing the internet. Users can store their files on MEGA and avoid having the files appear on their computer. Anyone searching an individual’s computer that utilizes MEGA would not be able to view these files if the user opted only to store them at an offsite such as MEGA. These are often viewed as advantageous for collectors of child pornography in that they can enjoy an added level of anonymity and security.

31. MEGA provides a variety of online services, including online storage access, to the general public. Dropbox allows subscribers to obtain accounts at the domain name <https://Mega.nz/login>. Subscribers obtain a MEGA account by registering with an email address. During the registration process, MEGA asks subscribers to provide basic personal identifying information. This information can include the subscriber’s full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

32. When the subscriber transfers a file to a MEGA account, it is initiated at the user’s computer, transferred via the Internet to the MEGA servers, and then can automatically be synchronized and transmitted to other computers or electronic devices that have been registered



with that MEGA account. This includes online storage in MEGA servers. If the subscriber does not delete the content, the files can remain on MEGA servers indefinitely. Even if the subscriber deletes their account, it may continue to be available on the MEGA servers for a certain period of time.

33. Online storage providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, online storage providers often have records of the Internet Protocol address (“IP address”) used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices accessed the account.

34. In some cases, MEGA account users will communicate directly with MEGA about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Online storage providers typically retain records about such communications, including records of contacts between the user and the provider’s support services, as well records of any actions taken by the provider or user as a result of the communications.

35. According to MEGA, Account Details are **voluntarily** disclosed to relevant authorities **without notifying the user** in all cases of alleged CSAM –(Child Sexual Abuse Material) or Violent Extremism storage / sharing – no Subpoena or MLAT procedure is

necessary. Foreign subpoenas or search warrants are irrelevant as Mega is incorporated in New Zealand and is not subject to foreign legal processes.

### **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

1. I anticipate executing this warrant to view and use the MEGA content that was downloaded from MEGA into a computer located in the FBI-Milwaukee Child Exploitation Task Force Office located at 3600 S. Lake Dr, St. Francis, WI 53235 in room 3260 “Innocent Images” as described in Attachment B under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A).

### **CONCLUSION**

2. Based on the foregoing, I request that the Court issue the proposed search warrant because there is probable cause to believe that evidence of a criminal offense, namely, a violation of 18 U.S.C. § 2252A, is located within MEGA account(s) associated with Macgwire Beck, which are more fully described in Attachment A, which is incorporated herein by reference.

3. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

## **ATTACHMENT A**

### **Property to Be Searched**

The property to be searched is the entire digital contents of the MEGA account(s) associated with the following:

MEGA's downloaded digital content of Beck's MEGA account –

Macgwire532@gmail.com located at the FBI –Milwaukee Office located at 3600 S. Lake Drive, St. Francis, WI 53235, Room 3260 “Innocent Images”.



## **ATTACHMENT B**

### **Particular Items to be Seized**

a. The contents of all folders associated with the account, including stored or preserved copies of files sent to and from the account, the source and destination addresses associated with file, and the date and time at which each file was sent;

b. All transactional information of all activity of the MEGA accounts described above, including log files, messaging logs, records of session times and durations, dates and times of connecting, and methods of connecting; and emails “invites” sent or received via MEGA and any contact lists.

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between MEGA and any person regarding the account or identifier, including contacts with support services and records of actions taken.

f. All information described above that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 2252A involving the account(s) associated with the MEGA account referenced in Attachment A pertaining to the possession and distribution of child pornography images and/or videos.